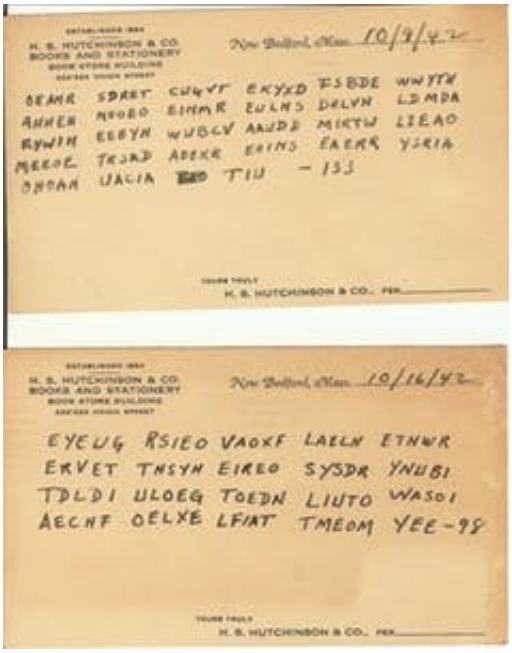
Is quantum computing a cybersecurity threat?

December 21 2018, by Dorothy Denning



Codes can be simple – or advanced. Credit: Derek Rose/flickr.com, CC BY

Cybersecurity researchers and analysts are rightly worried that a new type of computer, based on quantum physics rather than more standard electronics, could break most modern cryptography. The effect would be to render communications as insecure as if they weren't encoded at all.

Fortunately, the threat so far is hypothetical. The quantum computers that exist today are not capable of breaking any commonly used encryption methods. Significant technical advances are required before

they will be able to break the strong codes in widespread use around the internet, according to a new report from the National Academy of Sciences.

Still, there is cause for concern. The cryptography underpinning modern internet communications and e-commerce could someday succumb to a quantum attack. To understand the risk and what can be done about it, it's important to look more closely at digital cryptography and how it's used – and broken.

Cryptography basics

At its most basic, encryption is the act of taking an original piece of information – a message, for instance – and following a series of steps to transform it into something that looks like gibberish.

Today's digital ciphers use complex mathematical formulas to transform clear data into – and out of – securely encrypted messages to be stored or transmitted. The calculations vary according to a digital key.

There are two main types of encryption – symmetric, in which the same key is used to encrypt and decrypt the data; and asymmetric, or public-key, which involves a pair of mathematically linked keys, one shared publicly to let people encrypt messages for the key pair's owner, and the other stored privately by the owner to decrypt messages.

Symmetric cryptography is substantially faster than public-key cryptography. For this reason, it is used to encrypt all communications and stored data.

Public-key cryptography is used for securely exchanging symmetric keys, and for digitally authenticating – or signing – messages, documents and certificates that pair public keys with their owners' identities. When

you visit a secure website – one that uses HTTPS – your browser uses public-key cryptography to authenticate the site's certificate and to set up a symmetric key for encrypting communications to and from the site.

The math for these two types of cryptography is quite different, which affects their security. Because virtually all internet applications use both symmetric and public-key cryptography, both forms need to be secure.

Breaking codes

The most straightforward way to break a code is to try all the possible keys until you get the one that works. Conventional computers can do this, but it's very difficult. In July 2002, for instance, a group announced that it had found a 64-bit key – but the effort took more than 300,000 people over four and a half years of work. A key twice the length, or 128 bits, would have 2^{128} possible solutions – more than 300 undecillion, or a 3 followed by 38 zeroes. Even the world's fastest supercomputer would need trillions of years to find the right key.

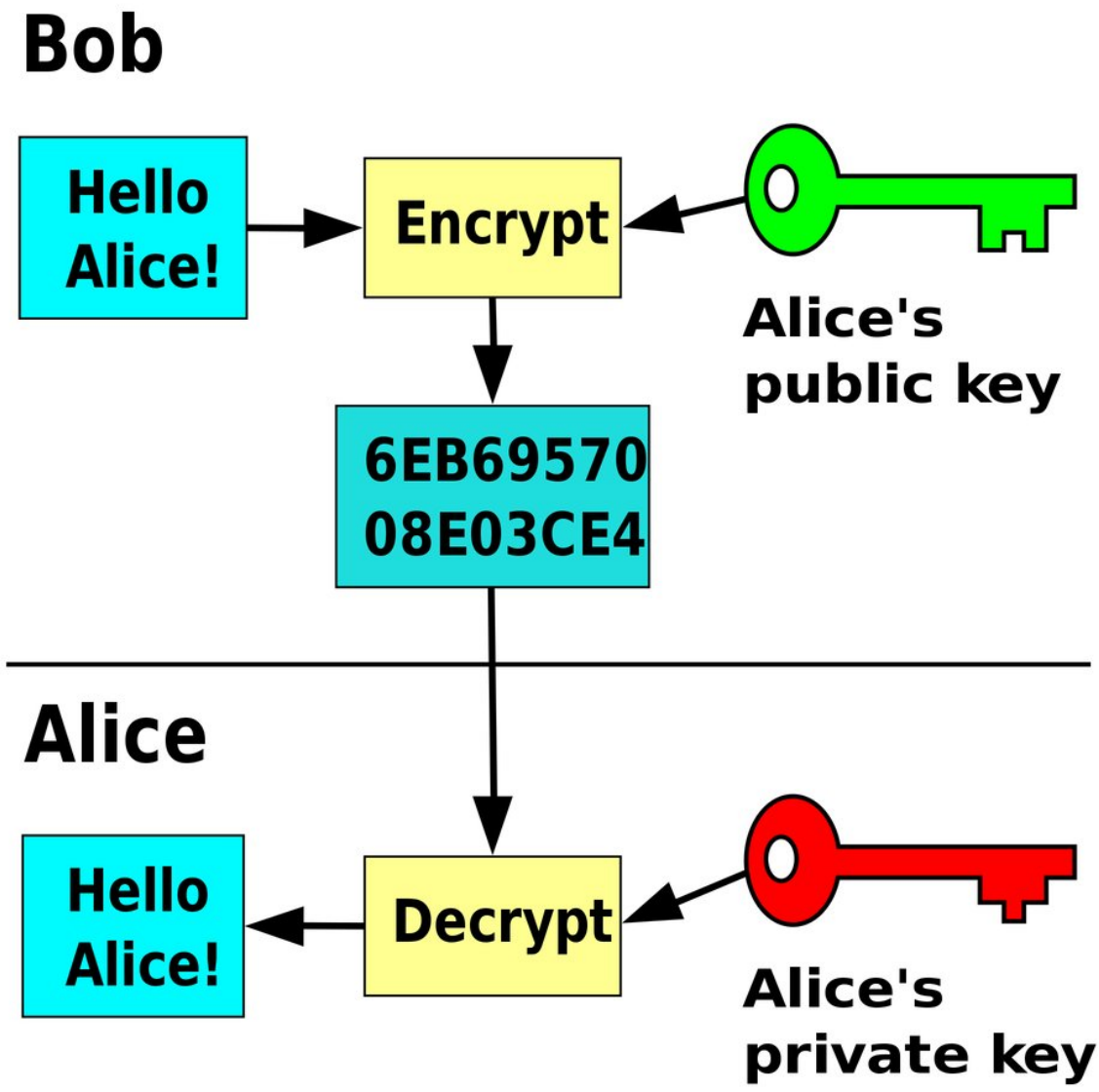
A quantum computing method called Grover's algorithm, however, speeds up the process, turning that 128-bit key into the quantum-computational equivalent of a 64-bit key. The defense is straightforward, though: make keys longer. A 256-bit key, for example, has the same security against a quantum attack as a 128-bit key has against a conventional attack.

Handling public-key systems

Public-key cryptography, however, poses a much bigger problem, because of how the math works. The algorithms that are popular today, RSA, Diffie-Hellman and elliptic curve, all make it possible to start with a public key and mathematically compute the private key without trying

all the possibilities.

For RSA, for instance, the private key can be computed by factoring a number that is the product of two prime numbers – as 3 and 5 are for 15.



A pair of keys can help strangers exchange secure messages. Credit: David Göthberg/Wikimedia Commons

So far, public-key encryption has been uncrackable by using very long key pairs – like 2,048 bits, which corresponds to a number that is 617 decimal digits long. But sufficiently advanced quantum computers could crack even 4,096-bit key pairs in just a few hours using a method called Shor's algorithm.

That's for ideal quantum computers of the future. The biggest number factored so far on a quantum computer is 15 – just 4 bits long.

The National Academies study notes that the quantum computers now operating have too little processing power and are too error-prone to crack today's strong codes. The future code-breaking quantum computers would need 100,000 times more processing power and an error rate 100 times better than today's best quantum computers have achieved. The study does not predict how long these advances might take – but it did not expect them to happen within a decade.

However, the potential for harm is enormous. If these encryption methods are broken, people will not be able to trust the data they transmit or receive over the internet, even if it is encrypted. Adversaries will be able to create bogus certificates, calling into question the validity of any digital identity online.

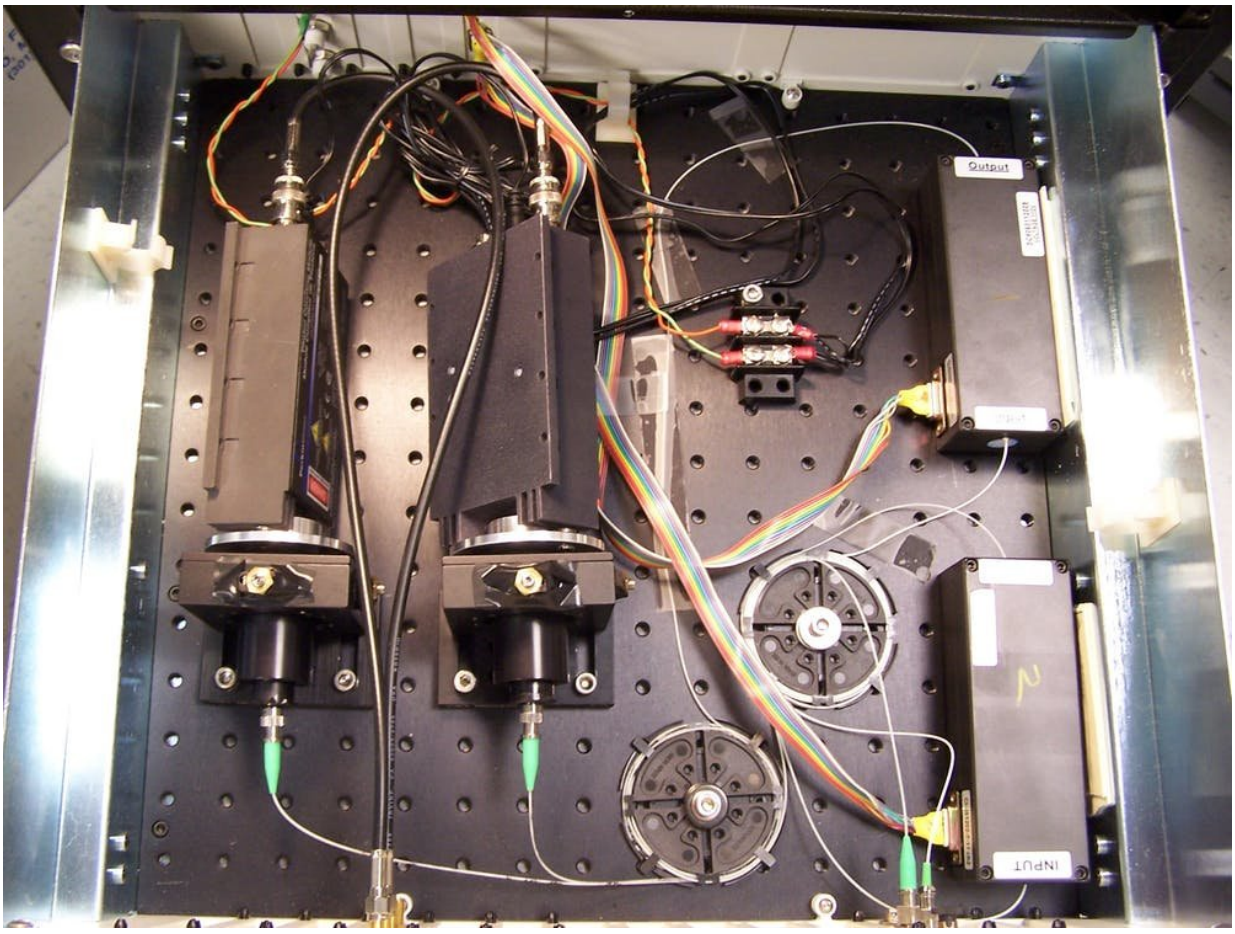
Quantum-resistant cryptography

Fortunately, researchers have been working to develop public-key algorithms that could resist code-breaking efforts from quantum computers, preserving or restoring trust in certificate authorities, digital signatures and encrypted messages.

Notably, the U.S. National Institute of Standards and Technology is

already evaluating 69 potential new methods for what it calls "post-quantum cryptography." The organization expects to have a draft standard by 2024, if not before, which would then be added to web browsers and other internet apps and systems.

In principle, symmetric cryptography can be used for key exchange. But this approach depends on the security of trusted third parties to protect secret keys, cannot implement digital signatures, and would be difficult to apply across the internet. Still, it is used throughout the GSM cellular standard for encryption and authentication.



A look inside a prototype of the hardware that exchanges quantum cryptography keys. Credit: National Institute of Standards and Technology/Wikimedia

Commons

Another alternative to public-key cryptography for key exchange is quantum key-distribution. Here, quantum methods are used by the sender and receiver to establish a symmetric key. But these methods require special hardware.

Unbreakable cryptography doesn't mean security

Strong cryptography is vital to overall individual and societal cybersecurity. It provides the foundation for secure transmission and data storage, and for authenticating trusted connections between people and systems.

But cryptography is just one piece of a much larger pie. Using the best encryption won't stop a person from clicking on a misleading link or opening a malicious file attached to an email. Encryption also can't defend against the inevitable software flaws, or insiders who misuse their access to data.

And even if the math were unbreakable, there can be weaknesses in how cryptography is used. Microsoft, for example, recently identified two apps that unintentionally revealed their private encryption keys to the public, rendering their communications insecure.

If or when powerful quantum computing arrives, it poses a large security threat. Because the process of adopting new standards can take years, it is wise to be planning for quantum-resistant cryptography now.

Provided by The Conversation